for that traffic class (e.g., policies, partitions, etc.). Administrator interface 150 also allows an administrator to manually create a traffic class by specifying a set of matching rules and, as discussed below, also automatically creates traffic classes by monitoring network traffic across access link 21 and classifying data flows according to a set of criteria to create matching rules for each traffic type.

Traffic class engine 136, in one embodiment, monitors network traffic passing through access link 21 and applies matching rules to identify a traffic class associated with each data flow. In one embodiment, traffic discovery engine 136 creates traffic classes automatically in response to data flows traversing bandwidth management device 30 and stores such traffic classes in traffic classification database 137. Automatic traffic classification is disclosed in application serial no. 09/198,090, now U.S. 6,412,000, which is incorporated herein by reference. In one embodiment, traffic class engine 136 must detect a minimum number of data flows for a given traffic type within a predefined period before it creates a traffic class in traffic classification database 137. As discussed above, administrator interface 150 allows for configuration of bandwidth utilization controls for auto-discovered and other traffic classes.

In one embodiment, traffic classes are configured to identify and segregate users into appropriate groups or categories and, thus, facilitate enforcement of volume-based network management policies. As discussed in more detail below, traffic class engine 136 applies matching rules to data packets based on IP address (or other suitable computer network address) to identify a traffic class associated with a particular user. In one embodiment, bandwidth management device 30 is configured to include traffic classes for known users, unknown users, and quarantined users. For example, traffic classification database 137 may include the following traffic classes: 1) /inbound/knownusers/, 2) /inbound/quarantined/, 3) /inbound/unknownuser/, as well as similar traffic classes for outbound data flows (e.g., /outbound/knownusers/, etc.). The matching rules associated with the /knownusers/ and /quarantined/ traffic classes are IP addresses, or other identifications added by user management server 44 to the configuration of bandwidth management device 30, as users register or exceed bandwidth utilization thresholds. In one embodiment, traffic class engine